

Information Technology Audit provides companies the confidence to identify and transform technology risk to a company's competitive advantage.

High-Value IT Audits

November 2009

*Powerful Insights.
Proven Delivery.™*

protiviti®
Risk & Business Consulting.
Internal Audit.



The Technology Landscape and IT Audit

- Technology is playing an ever-growing role in how organizations achieve their business objectives. In this environment it is increasingly important to assess appropriately technology vulnerabilities and risks as they relate to critical business processes.
- An organization's top executives, board of directors and audit committee members look to IT management for effective oversight of IT risks. The controls in place to manage these risks are an essential part of the internal control environment and structure.
- These same executives look to Internal Audit to evaluate whether IT risks are appropriately understood, managed and controlled.
- There are a number of IT audits frequently selected by audit committees, chief audit executives and others in the organization for their annual plans, which they consider to provide high value.



Defining High Value IT Audits

High Value IT Audits are designed to provide the audit committee and process owner with cutting-edge insights into the technology risks and related recommendations in the area under audit. The high value audit delivers actionable findings that drive the improvement of the organization's financial and business systems and business operations.

High Value IT Audits have two attributes:

- Audits having a high value proposition to the audit committee and internal audit leadership (know and recognize your risks).
- Audits that have a high value to the auditee because there is value in the observations, findings, and improvement opportunities, or the auditee is provided with valuable feedback as to their condition (process maturity insights).

Examples of High Value IT Audits

IT Governance and Management	IT Risk Assessment and Planning	Security and Privacy
<p>IT Governance</p> <p>IT Alignment with Business Strategy</p> <p>Project/Portfolio Risk Management</p> <p>IT Compliance Management</p> <p>IT Performance Management and Metrics</p>	<p>IT Audit Scoping and Risk Assessment</p> <p>CobiT Implementation Assistance</p> <p>Integrated Risk Assessments</p>	<p>Data Privacy</p> <p>Identity Management</p> <p>Database Security</p> <p>Financial Services Integrated Risk Assessment</p> <p>Payment Card Industry (PCI)</p> <p>Network Security</p>
Technology Infrastructure, Technology Components and Configurations	Information Strategy, Records and Data Management	IT Processes and Operations
<p>Operating System Architecture</p> <p>Database Architecture</p> <p>Network Architecture</p>	<p>Business Intelligence Diagnostic</p> <p>eDiscovery Readiness</p>	<p>IT Infrastructure Library Benchmarking</p> <p>IT Asset Management</p> <p>IT Service Management</p> <p>Process Benchmarking – ITPI</p> <p>Technology Change Management</p>
Services Continuity	Application Security, Controls and Configuration	
<p>Business Continuity Management</p> <p>Disaster Recovery Planning</p> <p>Crisis Management/Pandemic</p>	<p>ERP Security Assessment</p> <p>Pre-Implementation Assessment</p> <p>Post Implementation Assessment</p> <p>Automated Business Process Controls</p> <p>Transactional Data Integrity</p>	

High Value IT Audit – eDiscovery Readiness

E-Discovery is the process of locating, retrieving and producing relevant and responsive electronic data or documents as evidence for use in financial investigations and/or litigation.

Spending on electronic discovery (eDiscovery) software technologies and services offerings is forecast to grow at more than 35% annually through 2011. When faced with litigation or investigations, corporations struggle with gathering and producing relevant electronically-stored information responsive to requests. As a result, they potentially subject themselves to reputation risk, significant fines and sanctions or criminal charges.

On average, “American businesses are spending between \$2.5 and \$4.0 million per year for e-discovery per billion dollars in sales... making e-discovery the largest controlled cost in American business.” – Cohasset Associates, 2005.

VALUE PROPOSITION

What You Can Do	Assist the organization in assessing their readiness for litigation or investigations search through electronically-stored information for items that may be responsive to requests.
Example Issue	An organization evaluated its records management program against it's ongoing compliance, operational, and technology needs. During the assessment a gap analysis of the records retention policy was identified which highlighted that records information needed to be compiled, the current state of records management processes documented and site-specific processes including overall record storage, retrieval, disposition programs, technology solutions, and legal hold capabilities evaluated.
Value Delivered	Through the audit, the organization was able to recommend specific improvements to the retention policy and processes dispersed throughout the organization. The organization identified that they were not ready to turn over documents electronically, as legally required, and will now develop a plan to better prepare for and respond to crises, including the uncertainties of legal and regulatory risks that can impact the viability of their businesses.
Indicators of Need	<ul style="list-style-type: none">▪ The organization struggles with gathering and producing relevant electronically-stored information responsive to requests.▪ The organization has faced fines, or sanctions.

High Value IT Audit – Project Risk Management

Project risk management assesses the risk management effectiveness and control environment of any level of project activity, from a single project to enterprise-wide project management practices.

The latest statistics from the Gartner Group state that “30% of IT projects never come to a fruitful conclusion. On average 51% exceed budget by 189% while only delivering 74% of the originally stated functionality”.

VALUE PROPOSITION

What You Can Do	<p>Provide the organization with the processes and tools to identify, address and mitigate risks related to the management, execution and control of projects. Help the organization to optimize the execution of project management.</p> <p>Project risk management reviews include:</p> <ul style="list-style-type: none">▪ Early Stage Project Management Review – a review of controls and processes developed and initiated by the project manager to control the project.▪ Project Health Check – an assessment of the health of a project at a point in time.▪ Pre-implementation Review – provide assurance that all necessary preparatory activities have been completed.▪ Post-implementation Review – assess success of project against the business case and evaluate lessons learned.▪ Project Management Office Review – a review of PMO governance, procedures and reporting.
Example Issue	<p>A retail organization conducted a project risk management assessment to determine areas of project success and areas where project management improvements could be made. Identified issues included conflicting SDLC methodologies, and inadequate planning in the areas of budgeting, technical requirement gathering, and staff retention.</p>
Value Delivered	<p>The organization identified:</p> <ul style="list-style-type: none">▪ Additional project costs resulting from untimely risk identification, changes in scope, mismanagement of issues, or mismanagement of schedules.▪ Operational failures affecting customer and / or vendor contracts, service level agreement, accurate invoicing.
Indicators of Need	<ul style="list-style-type: none">▪ Organization is initiating or executing new projects.▪ Project is running late and deliverables keep growing.▪ Continuous scope creep suffered in previous projects.

High Value IT Audit – IT Governance

Executives across industries are becoming increasingly concerned about the communications, checks and balances between their business operations and their IT organization in order to align IT investments and priorities with business objectives. In some cases, IT costs are increasing, business needs are not being met, projects are failing and the technology is generally not providing enough value to the organization.

VALUE PROPOSITION

<p>What You Can Do</p>	<p>The primary objective of the IT Governance review is to review the effectiveness of an IT organization and identify opportunities to enhance the operational efficiency of IT through improved governance.</p> <p>An IT Governance assessment enables understanding of an IT organization’s alignment with the business through four key areas:</p> <ul style="list-style-type: none"> ▪ Strategy – the identification of key success factors for each of the organization’s operations and associated key performance indicators for IT; ▪ People – organization design with consideration for sourcing, skill needs, accountability, and business integration; ▪ Process – definition of IT service areas and an SLA based service delivery approach; and ▪ Technology – evaluation of technology assets in relation to current and planned operational needs, as well as the development of a standard technology and application architecture.
<p>Example Issue</p>	<p>A construction company found that IT investments did not align with the objectives of the organization and performed a review of their IT Governance to identify the underlying cause.</p>
<p>Value Delivered</p>	<p>The observations and recommendations delivered in the IT Governance report have resulted in IT redefining its role within the organization. Significant gaps between how IT viewed itself and how the business viewed IT were uncovered that led to a new IT organization structure and common expectations between IT and the business.</p>
<p>Indicators of Need</p>	<ul style="list-style-type: none"> ▪ IT investments are not aligned with the objectives of the organization. ▪ IT costs are increasing significantly year on year. ▪ IT projects are failing to deliver the expected benefits to the organization.

High Value IT Audit — Payment Card Industry (PCI) Compliance

In a climate of growing concern for identity protection, leading bankcard institutions have initiated programs to ensure cardholder information is safe. As a result of collaborations between Visa, MasterCard, American Express, Discover Card and JCB, the Payment Card Industry (PCI) Data Security Standard (DSS) was created.

Organizations that store, process or transmit credit card data are required to comply with the PCI DSS. The complexities of most hospitality companies can lead to an intricate and costly remediation process. Additionally, the process of achieving compliance with the PCI standard does not by itself guarantee safety from a costly breach.

VALUE PROPOSITION

What You Can Do	<p>Assess compliance to the PCI procedures and to ensure that the company is being assessed at the right level. The PCI audit can include:</p> <ul style="list-style-type: none"> ▪ Compliance Readiness Evaluation – help the organization position itself for successful completion of a Report on Compliance (ROC) by identifying systems that process or store data and ensure that appropriate controls are in place; ▪ PCI Remediation Assistance – Improve the efficiency and effectiveness of PCI-related procedures and controls to build a sustainable process for ongoing compliance with the PCI DSS; ▪ Ensure that mandatory PCI Assessment, Pen Test and Quarterly Scan are being performed.
Example Issue	<p>Large retail organization identified that a detailed review of infrastructure was necessary to ensure that the storage, processing and transmission of credit and debit cardholder data met PCI DSS standards, and that remediation plans could be put in place to resolve the issue quickly.</p>
Value Delivered	<ul style="list-style-type: none"> ▪ A thorough assessment of the effectiveness of controls across the systems and networking equipment that store, process or transmit credit and debit cardholder information, in respect to the 12 high level key requirements of PCI DSS. ▪ The internal audit of the PCI DSS at this organisation found 3 critical areas to be addressed, those of: Prohibited PCI Data, Vulnerability Scanning and Penetration Testing and Insecure storage of PCI Data.
Indicators of Need	<ul style="list-style-type: none"> ▪ Accept credit cards on a website, via e-mail or by fax; ▪ Point-of-sale (POS) systems are not certified as PCI-compliant by Visa; ▪ Business partners or service providers have access to organization’s customers’ credit card information; and ▪ Have had a security breach.

High Value IT Audit – Data Privacy

Publicized security breaches are at an all time high. Compromise of confidential data can cost millions in response costs, regulatory criticism, fines, and other penalties as well as irreparable reputation damage. Many organizations do not even know what confidential data they hold, where it is, or how it is protected. Data privacy services help organizations answer these questions and put controls in place to avoid costly incidents.

VALUE PROPOSITION

What You Can Do	<p>Data privacy audits are designed to help organizations identify confidential data on their network, determine if adequate controls are in place to use, share, store, protect and destroy data; identify potential root cause issues and provide recommendations for protecting data.</p> <p>Data privacy audits should consider personally identifiable information (PII) as well as laws, regulations, and industry standards, including but not limited to PCI, GLBA, HIPAA, State Breach Laws, and the European Union Data Directive.</p>
Example Issue	<p>A multi-phased data privacy audit was undertaken for a Bank. Activities included benchmarking the client data privacy and information security program against the requirements defined in GLBA 501b, testing portions of the program through investigation and evaluating the configuration of the supporting technology environment through external and internal penetration analysis.</p>
Value Delivered	<p>This review allowed the Bank to identify areas that required improvement and address those areas to be fully prepared for their upcoming regulatory review. The regulator was pleased with the proactive stance of the organization and as a result of implementing recommendations and making other enhancements to their security program, the organization was able to avoid repeated regulatory findings.</p>
Indicators of Need	<ul style="list-style-type: none">▪ Customer data has been stolen or lost by the organization.▪ New data privacy legislation is introduced.▪ The organization has an upcoming regulatory review and require assistance with preparedness.

High Value IT Audit – Identity Management

Identity Management facilitates and controls users' access to critical applications and resources. It promotes the notion of a holistic security environment which takes into consideration the people, processes, and technological dimensions of information security based on a risk-balanced, business-based approach.

"The connected computer is fast approaching ubiquity. We've created cyberspace, but we haven't yet really colonized it because we lack the organizing principle to do so. Having abolished time and space, nothing remains but identity. How we protect our identities into cyberspace is the central riddle. Until we solve that, we can't move on." - John Udell, InfoWorld

VALUE PROPOSITION

What You Can Do	<p>Identity Management solutions are varied based on the needs of the organization and may include</p> <ul style="list-style-type: none"> ▪ User access reconciliation; ▪ Identity management assistance; strategy and roadmap; requirements review; etc. ▪ Vendor analysis and selection.
Example Issue	<p>The Identity Management audit can help companies uncover excesses spending and to streamline a companies existing user account management processes. In addition, the audit will assist a company in understanding how sensitive information and brand reputation could be compromised by unauthorized users. In one audit, we identified savings of approximately \$1 million for each 10,000 users administered per year.</p>
Value Delivered	<p>The identity management audit assists companies in understanding its processes to add, change and delete users to/from their applications and systems. This audit helps companies identify savings opportunities and uncover potential exposures of confidential data through inefficient and insecure account management and application access processes.</p> <p>For companies where we have executed these audits, the cleanup of provisioning processes allowed for centralization and reduction of support staff and an auditing vehicle is now in place to monitor and maintain SOX compliance through timely activation and deactivation of user accounts and resolution of segregation of duties conflicts.</p>
Indicators of Need	<ul style="list-style-type: none"> ▪ It is difficult to quickly identify if terminated users still have access to systems. ▪ You cannot rapidly identify who has access to what systems and who owns what assets. ▪ Users have multiple user IDs and passwords for various enterprise systems managed by different administration. ▪ The organization does not have defined processes for requesting, approving and granting user access to applications.



Questions / Comments?

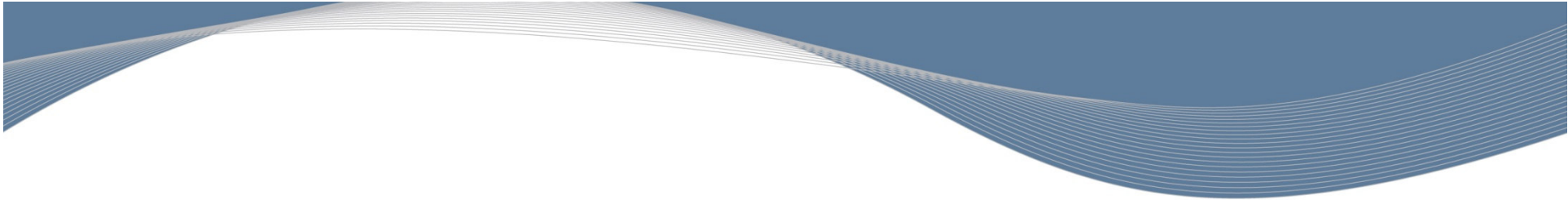
Mario D'Alicandro

protiviti[®]
Risk & Business Consulting.
Internal Audit.

1290 Avenue of the Americas
Floor 5 · Suite 503
New York, NY 10104
Direct: 212.399.8612
Fax: 212.399.8719
Mobile: 718.753.1032

Mario.DAlicandro@Protiviti.com

Powerful Insights. Proven Delivery.[™]



*Powerful Insights.
Proven Delivery.™*



Confidentiality and Disclosures

"This presentation contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly owned subsidiary of Robert Half International Inc. ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public."